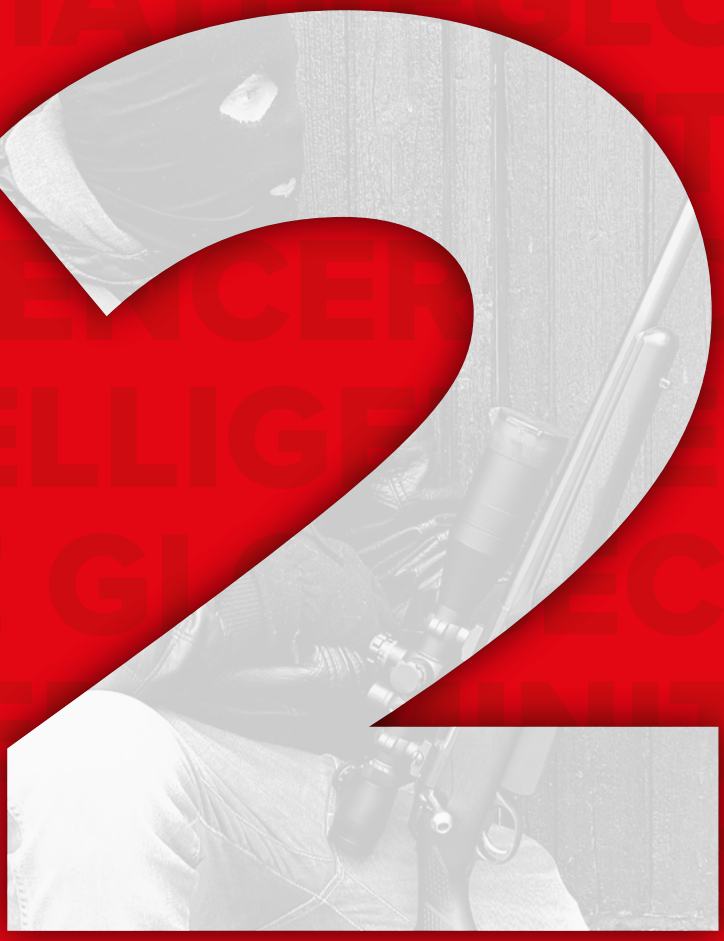

GLOBSEC INTELLIGENCE REFORM INITIATIVE

Towards a Transatlantic Counter-Terrorism Centre of Excellence

www.globsec.org

GLOBSEC
POLICY INSTITUTE

GLOBSEC Intelligence Reform Initiative

Towards a Transatlantic Counter-Terrorism Centre of Excellence
A Feasibility Study

May 2017

Steering Committee and Advisors

Hon. Michael Chertoff (Chair), former Secretary of US Department for Homeland Security, co-founder and Chairman of The Chertoff Group.

John Cuddihy, former Detective Chief Superintendent, Police Scotland, Visiting Practice Fellow at Coventry University.

Iulian Fota, former National Security Advisor to the President of Romania and Director of the National Defence College of Romania.

Dr. Kjetil Anders Hatlebrekke, Associate Professor of Intelligence, The Norwegian Defence Intelligence University College, and Senior Visiting Research Fellow, Department of War Studies, King's College London.

Professor Sir David Omand GCB, Visiting Professor, Department of War Studies, King's College London and former Director of the Government Communications Headquarters (GCHQ).

Dr. Cees Wiebes, intelligence scholar and former senior analyst at the Expertise & Analysis Department at the Office of the National Coordinator for Counter-Terrorism (NCTb) in the Netherlands.

Report Authors

Dr. Patrick Bury is a former infantry officer and Lecturer in Security Sector Management at Cranfield University, the Defence Academy of the United Kingdom.

Daniela Richterova is doctoral candidate at the Department of Politics and International Studies, University of Warwick, United Kingdom.

Table of Contents

1. Executive Summary

In 2017, terrorist attacks in Europe, the United States as well as in other parts of the world have continued. Mostly inspired by ISIL – the so-called Islamic State in Iraq and the Levant – these attacks indicate that this organisation retains the intent and capability to cause further harm.

As we argued in the GLOBSEC Intelligence Reform Initiative's (GIRI) last report, *Reforming Transatlantic Counter-Terrorism*, the recent terrorist attacks have revealed major seams in some nations' law enforcement and intelligence capacities and capabilities, and highlighted failures in both domestic and transnational counter-terrorism (CT) cooperation. Many of the failings identified occurred due to problems with standardisation, legislation, and organisational trust. Our last report proposed four solutions to improve transatlantic CT cooperation and national capabilities: the establishment of a permanent Core Transatlantic Counter-Terrorism Hub; operational Case-Based Task Forces; and a "hit no-hit" single search interface between existing databases. Our final recommendation was to create a transatlantic Counter-Terrorism Centre of Excellence to accelerate tactical and operational standardisation.

This feasibility report takes up the mantle of the CT CoE to explore the benefits of such a new body. The ultimate aim of the CT CoE would be to assist European and transatlantic partners in increasing their capacity, interoperability and trust. First, it would do so by creating a secure space to build and consolidate transnational and inter-agency relationships amongst mid-level CT professionals. Second, the CT CoE would provide a comprehensive practical training program for mid-level CT intelligence, security and law enforcement professionals from willing and capable states. This training would seek to contribute to standardisation in respect to terminology, threat assessment, protection of information and privacy as well as key tradecraft skills within the CT domain. The CT CoE would be a platform where best practices are exchanged, syllabuses and training material shared, and relevant courses introduced.

Based on our research, we propose that an already existing, respected CT institution should sponsor the CoE; that a respected framework nation provides the political will and expertise to ensure its success; that individual courses rotate through other respected nations; and that the courses become accredited by academic institutions. In doing so, the credibility of the CoE will be assured while the CoE itself can act as a gatekeeper for any CT Hub.

Intelligence cooperation is characterised by a high degree of informality and driven by personal relationships. The proposed CT CoE is not an attempt to change this informal culture. Furthermore, we acknowledge that it is neither possible nor desirable to dictate the standards of the intelligence, security and law enforcement profession to partner countries. Nevertheless, as discrepancies between states do exist, it is important to understand them and to create a voluntary platform for exchanging and potentially adopting practices from different intelligence and security cultures that best address the current terrorist threat.

If intelligence agencies do not continuously innovate and adapt to meet the increasingly transnational, criminal and technologically-savvy terrorists of today, the attacks of the past three years will continue. Moreover, by increasing trust amongst core nations' mid-level security personnel, a CT CoE would be conducive to flattening the hierarchical and stove-piped nature of transnational trust frequently concentrated around the most senior personnel. In short, by targeting adaption from the bottom up, a CT CoE will enable the organic development of a CT network amongst trusted partners. Our CT CoE recommendation is therefore an adaptive change, with low organisational and political risk, and relatively easy to establish in terms of resources and political capital. Thus, it promotes standardisation and trust through regular, formal training and education. It also represents the low hanging fruit of transatlantic CT reform: it is the easiest to do, with large potential gains for little risk. Crucially, it provides an opportunity to begin reforming transatlantic CT from the bottom up.

2. Introduction

Since the GIRI's last report, *Reforming Transatlantic Counter-Terrorism,* was released in November 2016, the European Union (EU) and the United States (US) have witnessed a further 12 major ISIL-related terrorist attacks. These latest attacks have killed 23 and wounded at least 186 civilians. As a result, between May 2014 and May 2017 at least 38 serious ISIL-related attacks have occurred inside the EU and US, killing 365 and wounding 1,243 citizens, over 275 of whom were critically injured. Attacks have occurred in the European capitals of Berlin, Stockholm and London, in major cities such as New York, New Jersey, Hamburg and Antwerp, and in Paris Orly airport. Meanwhile, Russia and Turkey have also suffered further major ISIL terrorist attacks. Clearly, the ability of ISIL-inspired terrorists to strike inside the transatlantic space and beyond has not diminished. As our last report identified, these terrorists are: increasingly linked with criminal networks; quickly self-radicalising online; less hierarchically organised; utilising more effective counter-intelligence techniques to evade detection; and using adaptive tactics to conduct both sophisticated and crude attacks.[1] The success of these recent attacks – in particular the fact that intelligence indicating their possibility were either not shared between nations or not prioritised – underscores the pressing requirement for improved counter-terrorism cooperation to respond to this constantly evolving threat. Indeed, as ISIL comes under increasing military pressure in Iraq and Syria, it is seeking to intensify its campaigns in the EU and US. Furthermore, the ongoing lack of integration of Muslim communities in both Europe and the US means this threat is likely to increase over time rather than diminish.[2]

Reforming Transatlantic Counter-Terrorism argued that a new transatlantic security architecture is needed to address the rise in Salafi jihadist terrorist attacks in Europe and the US. These attacks have exposed major loopholes in some nations' security architecture and highlighted that counter-terrorism cooperation could be more integrated at the transnational level to address the 21st century terrorist threat. In particular, our report proposed four solutions based on current best practices to improve transatlantic counter-terrorism cooperation and national capabilities. Our first proposal called for the establishment of a permanent Core Transatlantic Counter-Terrorism Hub would provide a secure space for linking existing national CT centres with high degrees of mutual trust. Secondly, within this Hub we recommended that operational Case-Based Task Forces be established, designed to react to current, emerging and residual CT challenges. Thirdly, the report recommended that a so-called "hit no-hit" single search interface be established to enable real time information exchange between already existing databases. Our final recommendation was to create a transatlantic Counter-terrorism Centre of Excellence (CT CoE) to accelerate tactical and operational standardisation in terminology, threat assessment, protection of information and privacy as well as key tradecraft skills within the CT domain. Consisting of willing and capable nations, this CT CoE would not only increase the capacity and compatibility of European and transatlantic CT partners, but would also help create a much-needed bridge between mid-level intelligence, security and law enforcement professionals on CT issues. Crucially, it would also help promote the social relations central to increasing organisational trust needed to improve transnational cooperation.

This feasibility report builds on our previous work, taking up the mantle of the CT CoE to explore the benefits of such a new body/network and how it could work effectively in practice. Centres of Excellence are not new in the security-counter-terrorism nexus; however, those networks established either nationally or as a part of wider alliances, such as NATO or the EU, have not initiated a comprehensive program targeting the practical training of mid-level CT intelligence and law enforcement professionals.

1 Globsec Intelligence Reform Initiative. (2016). *Reforming Transatlantic Counter-Terrorism,* Bratislava: Globsec, 12.

2 Interview, former national CT coordinator, 11 April 2017.

3. Context

In order to achieve truly professional operational cooperation, discrepancies among European and transatlantic partners in respect to standardisation, capacity and skill must be recognised and addressed. The post-9/11 world amplifies these discrepancies. Recent developments within the CT sphere have, according to former GCHQ officer Michael Herman, emphasised 'the importance of professional qualities throughout [the] whole process of collection, evaluation, assessment and distribution'. He adds that the importance of standards 'spreads well beyond the English-speaking communities' and that 'the era of increased inter-governmental cooperation increases the need not only for intelligence exchanges, but also for professionalism in handling it.'[3] Similarly, standardisation also contributes to defining and overseeing legal parameters for intelligence operations.[4] According to the former Director of GCHQ, David Omand, these developments could be facilitated by more 'rigorous intelligence community training' and more engagement between intelligence communities and outside experts.[5]

Recognising that a lack of standardisation is therefore a long-standing problem, this study argues that the time is ripe to invest effort and resources into addressing these discrepancies by establishing a Centre of Excellence for willing and capable member states (MS), which would assist European and transatlantic partners in increasing their capacity and interoperability in a practical manner. Firstly, this study explores the issues of trust and social relations, which the CT CoE seeks to address. Secondly, it briefly assesses the current CT intelligence, security and law enforcement training and education architecture. Finally, we present our CT CoE proposal that addresses these shortcomings and offers practical, bottom-up solutions.

3 Herman, M. (2004). 'Ethics and Intelligence after September 2001', ch. 12 In: Scott, L. and Jackson, P. D. (eds.). Understanding Intelligence in the Twenty-First Century: Journeys in Shadows. London: Routledge. 187.

4 Svendsen, A.D.M. (2012). The Professionalisation of Intelligence Cooperation: Fashioning Method out of Mayhem. Basingstoke: Palgrave, 24.

5 Omand, D. (2013). 'The cycle of intelligence'. In: Dover, R., Goodman, M.S. and Hillebrand, C. (2013). Routledge companion to intelligence studies. Routledge, 69.

4. Trust and Social Relations

Further ISIL-inspired attacks against soft targets inside the transatlantic space will provide a major challenge for its intelligence and security architecture as currently configured. Our previous report highlighted numerous functional and capability gaps in this architecture, many of which, despite some recent improvements, remain problematic. The most important of these include professional trust and practical transnational cooperation between different nations' intelligence and law enforcement agencies at all levels of the intelligence cycle. Recent attacks have shown that there are wide discrepancies between European states' intelligence as well as law enforcement capabilities and capacities, and that some of the most capable nations remain reluctant to share with less capable nations due to well-founded scepticism about their operational capabilities and, crucially, their ability to prevent leaks. Similarly, there needs to be trust that if a specific piece of intelligence is passed on, it is not acted upon without the originator's consent and in reference to their legal framework. Whilst numerous legislative and historical discrepancies between some nations further inhibit trust-building, it must also be recognised that some bilateral intelligence sharing relationships, and indeed core multilateral arrangements such as Five Eyes Plus, work very well and have very high degrees of trust complimented by strong organisational security cultures. On the other hand, it is also clear that the WikiLeaks and Snowden revelations damaged transnational trust and some bilateral relationships.

The problem of trust also manifests itself at the domestic inter-agency level, and especially between law enforcement and intelligence services. In particular, the Paris and Brussels attacks of November 2015 and March 2016 highlighted that numerous European intelligence, law enforcement, security and legal services have not succeeded in developing a strong sense of a communal counter-terrorism effort. Despite some efforts to centralise and improve sharing, some nations' security services remain functionally divided, curtailed by rivalry, and reportedly under-resourced. They therefore do not share information with each other – or with their governments – to the same degree as more capable nations that have adopted the Fusion Cell/Hub model. As a result, they can struggle to share information rapidly in order to identify and pre-empt attacks. As many of the perpetrators of recent terrorist attacks had criminal backgrounds, the failure to fully incorporate law enforcement into the national CT effort has also left operational and tactical cooperation gaps and curtailed some nations' ability to collect valuable human intelligence (HUMINT) from often marginalised communities. Without stronger trust between intelligence and police agencies, this is likely to continue.

4.1 Legislation

Inevitably however, some restrictions on sharing information between intelligence, security and law enforcement must remain in place. Sharing intelligence with law enforcement is sensitive and must follow strict rules and regulations in accordance with national legal safeguards, including whether certain intelligence can be used in court. National legislation is not the only obstacle. On a more fundamental level, the problem stems from the fact that intelligence starts with uncorroborated hints and leads. That is why intelligence services are usually denied executive power: if this 'principle of suspicion' is to be transferred to law enforcement, it must be closely regulated. Otherwise it can lead to flawed procedures, violation of fundamental rights, misuse of powers or eventually to a secret police system. This challenge also translates to international intelligence, security and law enforcement cooperation. According to veterans of European intelligence services, creating legally acceptable cooperation channels between intelligence and security networks such as the Club de Berne's Counter-Terrorism Group (CdB CTG) and its law enforcement counterparts such as Europol is a challenge that will need to be overcome.[6]

4.2 Culture

Closely related to whether national intelligence agencies trust one another are the issues of capability and security culture. Capability discrepancies across a number of functions essential to strong CT

6 Interview, 5 April 2017, Brussels.

cooperation can, and are, curtailing transnational trust. Not all services are known to follow CT case management and prosecution best practices when handling intelligence or personal information.[7] The issue of the actual capability of intelligence operatives is also key as it determines whether an intelligence agency can be relied upon to conduct covert missions and collect vital intelligence without revealing itself and potentially damaging wider investigations. Partners' collection capacity is also important: do these intelligence and law enforcement services have a broad spectrum of strong HUMINT, signals intelligence (SIGINT) and protected information (PROTINT) collection capabilities, or are they skewed to certain areas, or not up to standard across these functions? Does their analysis, dissemination and operational functions work effectively? Moreover, do their intelligence services have strong democratic oversight and do politicians hold them accountable? Does their legislation allow them to act on the intelligence and/or information being sent from internal/external allies? Similarly, and often most importantly, how strong is the security culture of the organisation receiving the intelligence? Is there rivalry between domestic agencies that would prevent the passage of information? Does an agency or agencies have a history of leaks, or are they politically too close to potential adversaries to warrant the risk of sharing? As such, there are numerous very practical considerations – which have often been learnt the hard way – that influence transnational and inter-agency trust.

4.3 Interpersonal Trust

It is therefore clear that trust is the fundamental foundation upon which good transnational and inter-agency CT cooperation is based. As one former senior CT professional admitted, 'trust is based on enhanced social relations.'[8] Thus, trust is an inherently social product. In counter-terrorism, trustworthiness is dependent on consistent and correct behaviour in past interactions, organisational mutual dependence and strong security cultures, but in its strongest form it is about relationships; the social cohesion found within and amongst organisations. The literature on social cohesion is informative here, as long-standing research on military groups has found it not only to be correlated with high degrees of trust, but also to effective group performance in high-stress situations.[9] It is therefore clearly relevant to practical trust between mid-level intelligence and law enforcement professionals. Moreover, often the strongest forms of transnational trust are based on interpersonal relationships and social cohesion between service heads that have been forged through shared experiences, a history of trustworthy interactions, and common values and language. It is no coincidence that the Five Eyes agreement was originally based around English-speaking nations, while other highly trusted partner nations such as Norway, Sweden and the Netherlands, traditionally have very strong English competencies throughout their services.

Further down the chain of command, especially at the domestic level, strong bonds of trust are created by shared experiences of operations and training, but, as we will see, this can be inhibited at the transnational level due to a lack of a multi-agency approach. **Creating a secure space to build and consolidate transnational and inter-agency relationships amongst mid-level CT professionals is therefore central to this report's emphasis on a CT CoE.** Building this trust will be reliant on the relevance of the subjects covered and the quality of the instructors and attendees, but also on the latter's ability to openly share experiences and discuss best practices. Only with such quality assurance, complimented by the interactions between mid-level intelligence and law enforcement officers from trusted partner nations, can a gradual increase in transnational trust from the 'bottom up' be effected.

7 Interviews, 27 March 2017, Norway; Interview, 3 April 2017, London.

8 Comments, former national CT coordinator, 12 October 2015.

9 Globsec Roundtable, Bratislava, 15 April 2016.

5. The Need for Standardisation

Experts and practitioners alike have expressed the need to increase standardisation in counter-terrorism. Issues with regard to standardisation have emerged in both old and new democracies. For instance, the UK – which today arguably represents Europe's best example of national standardisation in CT intelligence practice – went through a steep learning curve as a result of Northern Irish terrorism and then the Al Qa'ida threat. Furthermore, analytic training was improved following the 2004 Butler Report on intelligence failures on Weapons of Mass Destruction that informed the decision to invade Iraq. Moreover, in its 2007 report on the practice of 'renditions', the UK's parliamentary oversight body – the Intelligence and Security Committee (ISC) – highlighted some of the problems associated with a lack of standardisation; 'Other countries have different legal systems and different standards of behaviour to the UK, and their intelligence and security services have varying levels of capability, capacity and professional standards. These factors must be taken into account when working with foreign liaison services.'[10]

Standardisation was also an issue within US intelligence. So much so that in 2005, a report published by the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction – also known as the Robb Silberman Report – suggested establishing a National Intelligence University to implement standard terms and practices. Although various discipline-specific intelligence training programs had been in place for decades, the Report recognised that there was no initial training provided to all incoming intelligence personnel that 'instils a sense of community and shared mission – as occurs, for example, in all of the military services'. Furthermore, the Committee thought that there was also lack of adequate management training programs, which arguably contributed to the declining numbers of mid-level intelligence officers.[11]

Since the fall of communism, some of the newer EU member states are also said to have inadequately trained their intelligence officers. Insufficient and unprofessional recruitment strategies, a lack of continuity caused by intelligence politicisation and purges of communist-era personnel, and poor operational planning skills which often result in improvisation have been identified.[12] However, other Eastern European countries argue that their training is more compatible with the US and UK models than that of some of the older Western European democracies. This paradox is a consequence of NATO's pre-accession training carried out throughout the region in the 1990s and early 2000s.[13] Overall, according to a former head of a continental European intelligence service, this variety of standards is also determined by their training capacities and on who intelligence agencies primarily recruit.[14] Indeed the lack of standardisation across the transatlantic space is so great that some veteran intelligence practitioners have suggested an audit of the methods, terminology and level of national standardisation among transatlantic partners.[15]

10 'Renditions Report'. (2007). Intelligence and Security Committee, UK. 13.

11 Iraq Intelligence Commission. (2005). 'Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction'. Unclassified Version, March, 31, 325-26.

12 Csipák, L. (2013). 'Únik utajovaných informácií z prostredia spravodajských služieb'. Asociácia bývalých spravodajských dôstojníkov. 41-2.

13 Interview with Iulian Fota, Director of National Intelligence College, 4 May 2017.

14 Interview, 5 April 2017, Brussels.

15 Interview, 27 March 2017, Norway.

6. International Networks and Training

Since 9/11, CT has become one of the most prominent issues on the agendas of intelligence and security agencies worldwide. Consequently, it has become a core issue to multiple intelligence, security and law enforcement alliances. As a reaction to the recent wave of terror in Europe, a number of these alliances are being re-assessed, upgraded and operationalised to fit this new security environment. Indeed, a number of these international networks have introduced training or exchange of best practices programs into their portfolio. To understand where and how the CT CoE could bring value or enhance and compliment the work of already existing programs, the following section briefly examines their capacities to conduct joint training of mid-level CT operatives and analysts. Existing networks without training functions are not discussed.

Current transatlantic counter-terrorism networks can be divided into those that broadly operate on the strategic, operational and tactical levels. Strategic intelligence, which is concerned with security trends and wider emerging threats and challenges, is generally less sensitive and shared more routinely; operational and tactical intelligence, which looks at specific leads and cases, is more sensitive and thus cooperation in this domain is less frequent and much more restricted.

6.1 Five Eyes

Arguably the most effective core transatlantic CT network, spanning both the strategic and operational levels, is the Five Eyes arrangement between the US, UK, Canada, Australia and New Zealand. Each of these countries – all Anglophone with common legal systems – provide different capabilities and geographical coverage, but the long-lasting relationship between members and their high levels of trust have proven conducive to the regular sharing of other types of intelligence. A number of more recent, subsidiary bilateral sharing agreements have reportedly been set up within the Five Eyes framework, such as the so-called Nine Eyes network, comprising Denmark, Norway, France, and the Netherlands. A wider alliance, the 14 Eyes Group – also known as SIGINT Seniors Europe (SSEUR) – expands this network to include Germany, Spain, Italy, Belgium, and Sweden. This alliance is predominantly focused on exchanging military SIGINT. However, while the Five Eyes network does foster close and frequent liaison, a degree of standardisation, and stronger trust between members, as far as we are aware this does not extend to regular and formalised joint training for mid-level CT officers and analysts.

Within the Five Eyes alliance, another well respected platform is the Leaders in CT (LinCT) network, which operates predominantly on the operational and tactical levels exclusively within the CT domain. It informally brings together law enforcement, intelligence services and the military from these nations to provide the basis for enhanced social relations and the cross fertilisation of ideas, best practices and experiences that build trust.[16] Rotating between member states, classified meetings are held each year that attract senior personnel. The quality of attendees, the frank nature of discussions, and the strong level of trust ensure that attendance is highly desired. However, it is open to top and senior, not mid-level, officials only. While LinCT does conduct some training on a rotational basis for Future Strategic Leaders, in reality these are also senior personnel. It does not currently conduct regular, formal, CT training for mid-level personnel and neither is its training accredited.[17]

6.2 Club de Bern's Counter-Terrorism Group

Within the European CT context, the CdB CTG is also well respected and of increasing importance. Established in 1971, the CdB consists of the heads of EU MS internal security services and those of Norway and Switzerland and it has traditionally dealt with strategic level intelligence. However, after 9/11 it set up the CTG to specifically address Salafi jihadist terrorism, and this has led to an increasing emphasis on operational and tactical cooperation. In establishing the CTG, the Club de Bern aimed to achieve a delicate balance by which, on one hand, they helped facilitate multilateral liaison and, on the other, kept intelligence competence and decision-making within the remit of the MS.

16 Comments, former national CT coordinator, 12 October 2015.

17 Interview, former national CT coordinator, 11 May 2017.

In 2016, in reaction to the terrorist attacks in Europe, the CTG strengthened its integration and tactical cooperation. Under the stewardship of the Dutch domestic intelligence and security service, the AIVD, members of the CTG launched an operative platform for multilateral exchange of operational CT-related information. Representatives from its MS are now meeting on a weekly basis to address some of the issues identified by the evolving jihadist threat. It also recently established its own database, the effectiveness of which is yet to be determined. In practice, however, some difficulties remain: to date, not all MS have appointed liaison officers to the platform; attempts at CT cooperation with some EU agencies, such as Europol, have had little success, with the CTG MS services giving preference to sharing information with their national law-enforcement bodies on a bilateral basis in accordance with national legislation.[18] Moreover, the CTG remains focused on operational matters; it does not coordinate standardisation of terminology and practice nor host regular, formal, training for mid-level intelligence and law enforcement officers.

6.3 INTCEN

The importance of standardisation and joint training has also been recognised by INTCEN, the EU's key strategic intelligence body, which also produces CT assessments and reports. Over the past decade, INTCEN production has moved from primarily working with open source intelligence (OSINT) and EU diplomatic reports, to producing fused strategic assessments based on MS civil/military, domestic and foreign intelligence reports, delegation reports, and OSINT. Efforts to centralise CT analysis within INTCEN are currently under way with plans to set up a larger CT unit. Increasing INTCEN's capacity by seconding more MS personnel is also under consideration, and, overall, the trend within INTCEN has been to gradually move from bilateral to multilateral liaison. However, the degree of multilateral sharing varies considerably between MS and is determined by history and political landscape.

Crucially, INTCEN has also invested in standardising tradecraft training. This is based on the INTCEN leadership's recognition of the importance of sharing standards (terminology, analysis and collection methods) in CT. This training is conducted by selected MS services to encourage the exchange of best practices. Intelligence scholars have also been engaged in this process. Moreover, in terms of capacity building, INTCEN tapped into the expertise of colleagues seconded from MS and turned these into a best practice manual. Moreover, INTCEN had organised training on intelligence utilisation for consumers, which was found to be a useful exercise. Reportedly, there is great appetite from policymakers, in MS as well as the European Commission, for briefings on the CT situation. The only major constraint to developing these programs further are issues of capacity.[19] Ultimately, INTCEN is an EU institution working with EU MS services and for the Union's policymakers. Linking a wider transnational initiative such as the CT CoE, which envisions engaging nations outside the EU, with INTCEN would therefore not be feasible.

6.4 EUROPOL

Europol was launched in 1999 to predominantly facilitate joint analysis and exchange of criminal intelligence on organised crime between all EU MS.[20] In January 2016, Europol established the European Counter Terrorism Centre (ECTC), which utilises new integrated databases and computer networks to store and exchange data between MS, and partners such as Interpol and Eurojust.[21] Although in the wake of the Paris and Brussels attacks Europol assisted in providing leads to the French and Belgian authorities, the ECTC is yet to prove its worth to MS intelligence communities, a number of which have been reluctant to share CT-related information via this platform as they have not managed to overcome the 'nation-centric culture', discussed above. There have been recent attempts to increase the ECTC's role in the CT domain and establish cooperation with the CTG, but without visible progress. Some MS representatives have argued that this is very much a symptom of the fact that this process is driven by heads of these organisations; it is not a bottom-up, organic phenomenon.[22] Based on available data, the Europol does not run any joint CT training programs for EU MS mid-level intelligence, security law enforcement and justice professionals.

18 Interview, 5 April 2017, Brussels.

19 Interview, 5 April 2017, Brussels.

20 Interview, 17 August 2016, Brussels

21 'History of Eurojust'. EUROJUST. http://www.eurojust.europa.eu/about/background/Pages/History.aspx, Accessed: 6 April 2016.

22 'Europol Review 2014: General Report on Europol Activities'. Europol. https://www.europol.europa.eu/content/europol-review-2014, Accessed: 10 March 2016; Interview, 4 April 2017, Brussels.

7. Existing Centres of Excellence

7.1 NATO

To date, various security or political alliances have adopted the Centre of Excellence model. For instance, NATO established its Centre of Excellence for Defence Against Terrorism in Ankara, Turkey, which serves as a hub for discussion on counter-terrorism. The Centre is said to conduct training and education – courses, seminars, conferences and workshops – on CT issues for NATO MS and partner countries, as well as cooperate with academic research. Nevertheless, it is unclear whether the intelligence, security and law enforcement professionals central to CT efforts are involved in these activities nor what skills these programs address.[23] Indeed, given that NATO is a military alliance unable to collect data on its own populations, its real domestic utility appears rather limited.

7.2 RAN

In 2015, the EU Commission established a Centre of Excellence within its Radicalisation Awareness Network (RAN). RAN was set up to target radicalisation by facilitating the exchange of expertise and best practices among so called 'first line practitioners', which include educators, social workers, local authorities and other actors relevant to the CT cause.[24] The RAN CoE's emergence two years ago suggests the increasing need for exchange of best practices and knowledge among CT professionals on the European continent.

7.3 GCTF

Since 2011, the Global Counter-Terrorism Forum (GCTF), initiated by Turkey and the United States, has brought together dozens of CT professionals to promote a joint strategic approach to CT and radicalisation. In concert with the UN this informal platform examines: effective responses to the 'foreign terrorist fighters' phenomenon; the role of the judiciary in adjudicating offenses related to terrorism; rehabilitation and reintegration of violent extremists; and community engagement and community-oriented policing as tools for countering violent extremism. It runs a number of courses aimed at exchanging best practices on how to deal with some of these challenges.[25]

7.4 The US

In the US, the Department of Homeland Security has also set up two centres of excellence focused on counterterrorism, in both instances these are led by established academic institutions. The National Center for Risk and Economic Analysis of Terrorism Events (CREATE), led by the University of Southern California, evaluates risk perception, communication and assessment. Moreover, it also evaluates the costs and consequences of terrorism.[26] The National Consortium for the Study of Terrorism and Responses to Terrorism (START), led by the University of Maryland, provides policy makers and practitioners with empirically grounded findings on the human elements of the terrorist threat and informs decisions on how to disrupt terrorists and terrorist groups.[27]

Clearly, transatlantic CT networks exist in both the intelligence and law enforcement domains. While these vary in respectability and effectiveness, they highlight that some of the most effective transnational cooperation is taking place within smaller alliances. Moreover, those involved in these networks are predominantly very senior intelligence personnel (service chief level). This reality shapes

23 'Centre of Excellence Defence Against Terrorism'. Coedat.nato.int, http://www.coedat.nato.int/about.html, Accessed: 24 April 2017.

24 'Radicalisation Awareness Network (RAN)'. Migration and Home Affairs - European Commission, https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network_en, Accessed: 25 April 2017.

25 'Global Counterterrorism Forum (GCTF)'. https://www.thegctf.org/About-us/Background-and-Mission, Accessed: 25 April 2017; NATO PA. (2016). 'FINAL REPORT - Enhancing Euro-Atlantic Counter-terrorism Capabilities and Cooperation'. Nato-pa.int, 8-9. http://www.nato-pa.int/default.asp?SHORTCUT=4320, Accessed: 25 April 2017.

26 'Center for Risk and Economic Analysis of Terrorism Events (CREATE)'. http://create.usc.edu/research/research-areas, Accessed: 25 April 2017.

27 'The National Consortium for the Study of Terrorism and Responses to Terrorism'. http://www.start.umd.edu/, Accessed: 25 April 2017.

wider international and inter-organisational trust in three ways. Firstly, there is a lack of participation by mid-level intelligence, and especially law enforcement officers, in many of these networks thereby excluding them from developing trust-based relationships until much later in their careers. This limits wider inter-organisational trust, especially when compounded by well-founded traditional counter-intelligence security cultures that often foster suspicion amongst the most able mid-level intelligence officers. Secondly, law enforcement CT networks are generally weaker than those in intelligence, despite the fact that policing is increasingly crucial to CT efforts. Finally, none of these networks are providing regular, formalised training to their members, and decisively, to mid-level officers, thereby failing to capitalise on their successes by regularly educating their best intelligence and law enforcement officers together to gradually build trust. In short, an opportunity to reform transatlantic counter-terrorism cooperation from the ground up is being missed.

8. National CT Training and Education Centres

On the national level, an increasing number of European states have introduced intelligence education and training institutions. The following section highlights some examples of countries, namely Norway, Romania and the Scotland, with institutions that run two-tier intelligence training and education: tradecraft-focused programs for entry level intelligence officers and wider educational courses for mid-level/senior officers aimed at increasing their general knowledge of intelligence and its relevance to politics and strategy. Discussions with representatives of these institutions suggest that there is considerable interest to share best practices in the CT tradecraft field internationally, which would encourage trust and standardisation at the international level.

8.1 Scotland

Scotland's recent experience of CT transformation is highly informative due to its implementation of standardisation and training in a multi-agency environment. It centralised eight regional police forces and two agencies in April 2013 in the new Police Scotland organisation and established a Scottish Crime Campus (SCC) outside Glasgow. In terms of CT policing, there was a requirement to ensure national standards of both operational and professional competence were being adopted and applied: 10 versions of the truth had to be fused together in order to create coherent and coordinated CT responses.

The underlying approach to standardisation and training was to promote a culture and behaviours that would epitomise the new organisation and deliver both internal and external trust in competencies. Effective governance was identified as key to this and as such, in the CT domain, CTOLD – Counter-Terrorism Organisational Learning and Development – was established. This was supported by the creation of a skills matrix to define what skills were needed in particular roles; what was the standard of training required in each role, and how such training would be delivered. This resulted in the matrix identifying every role required, the professional and personal competencies required, and the appropriate accreditation. Interestingly, this skills-based analysis resulted in the introduction of inputs at the CT recruitment stage to support organisational cultural change from the bottom up.[28]

Basic training was delivered at the Scottish Police College and at UK facilities to ensure that interoperability, governance, standards and tradecraft were comparable. This training also enhanced social relations and built inter-agency trust. The training extended beyond rank and file to involve Counter-Terrorism Senior Investigating Officer training, and at the mid-level, Counter-Terrorism Police Operations Room manager training, Intelligence Manager training and analyst training. There was a 'golden thread' in all training courses to ensure a single version of the CT intelligence picture was formed, underpinned by standardised terminology and practices. This training was then expanded into a multi-agency context – law enforcement, military and intelligence partners engaged in table-top and live play exercises- and then further training to ensure interoperability and the understanding of roles and responsibilities. This enhanced trust and confidence through the mutual exchange of information. In terms of CT, a single intelligence data platform was also introduced requiring multi-agency training to ensure common language, common standards, and common tradecraft in intelligence handling. This included law enforcement and intelligence services, UK Border Force, military, fire service, the National Domestic Extremism and Disorder Intelligence Unit, Civil Nuclear, and customs and immigration agencies.

When gaps in operational competency are identified through CT operational debriefs, they are referred to CTOLD who then allocate ownership with leads in training, policy, and legislation to ensure the lessons learned are incorporated into future training and education. This process continues by fusing assets from academia, third and private sector. If CTOLD identifies a gap in learning requiring academic input, a university can be approached to carry out appropriate research. This process has already benefited academia with rich data and law enforcement with rich thinking that can then be operationalised on completion. In addition, those officers and staff with a particular aptitude for further education are sponsored by a university to undertake a PhD in areas of operational importance.

28 Comments, former CT professional, 10 May 2017.

This fusion of learning and education led to the creation of multi-agency governance groups and the delivery of Police Scotland CT training with multi-agency assets. The result has been safer, stronger communities; a flexible and agile multi-agency CT workforce with the confidence and trust in one another to enhance information exchange, and the coordinated sharing of assets resulting in a greater level of actionable intelligence. The multi-agency training has now extended upwards within the organisation with senior commanders regularly participating in joint exercises and, more importantly, strengthening their relationships thereby making it easier to exchange information ahead of a critical incident.

Overall, the creation of the SCC delivered organisational change, created stronger governance mechanisms, national standardisation, improved relationships and enhanced trust. It has resulted in the right people with the right skills being deployed at the right time against the threats, which allows for appropriate resource allocation against the demand profile. Due to its success, the SCC has grown to include 19 national agencies, and is internationally recognised as a Centre of Excellence.

8.2 Norway

A frequently cited example of national level best practice in intelligence and CT training and education is the Norwegian Defence Intelligence University College. The mission of the centralised, multi-agency University, which belongs to the Norwegian Foreign Intelligence Service (NIS), is to 'serve and build the intelligence community through research, teaching and doubt.'[29] Building on its academic expertise, it has adopted an overarching cognitive approach to both teaching and research. As a result, understanding and assessing validity and reliability in the intelligence process are fundamental to the University's teaching.

In terms of education, the University delivers two, three-year Bachelor of Arts (BA) degrees in intelligence. The first degree is part time and is designed for mid-level intelligence officers, analysts, decision makers and, importantly, consumers. This accredited educational course aimed at mid-level practitioners is especially relevant to a potential CT CoE in terms of how it could deliver wider educational benefits. The students come from the foreign and domestic intelligence services, as well as the wider intelligence community, including Special Forces. The objective of the course is to give students the opportunity to reflect more broadly on their trade as their careers progress. As such, it fuses academic and professional knowledge of intelligence through the combination of both. Course modules include judicial and legislation issues; intelligence history; functional approaches to intelligence; structural approaches to intelligence; decision-maker support; and intelligence leadership. The course is designed to allow these mid-level producers and consumers of intelligence to refresh their skills and thereby bring decision makers and the services closer together.

In line with other national intelligence and CT institutions, the University also runs a BA in Intelligence and Languages for entry-level officers and numerous tradecraft and analysis courses at the more senior second and third levels. Other major European nations have praised the University's ability to centralise multi-agency intelligence and CT intelligence training in one location whilst at the same time fusing academic and practitioner best practice. Whilst it must be recognised that because Norway's intelligence service and its military intelligence are controlled by the Ministry of Defence this fusion is somewhat easier, and that the relatively small size of Norway's intelligence/CT community is another factor, it is highly regarded both domestically and at the international level.

8.3 Romania

The intelligence education model promoted by the Romanian Intelligence Service via its 'Mihai Viteazul' National Intelligence Academy (MVNIA) represents one of the most advanced of its kind in the former communist countries of South Eastern Europe. The Academy, established in 1992, delivers a variety of widely-respected educational programs; BA, MA, and advanced vocational training.

Of most relevance to the CT CoE proposal are the Academy's BA level courses dedicated to the future officers of the SRI, the Romanian Domestic Intelligence Service. These cadets can either develop their analytic skills by enrolling in the Security and Intelligence Studies program, or become case officers and enrol in the Psychology – Intelligence program. Courses include logic and argumentation theory

29 Interview, 27 March 2017, Norway.

(critical thinking), information security management, human behaviour optimisation techniques, foreign languages and strategic influence operations, applied informatics in intelligence activity. Future case officers undergo training in psychology: the psychological assessment of the individual and the group, training in networking, motivation and interpersonal communication.

Of further interest are the Academy's mid-career programs, run by the National Intelligence College, which provide post-graduate education to a wide variety of mid-level from military, intelligence and law enforcement professionals, to relevant government civil servants to consolidate their strategic decision making skills. The three-month long course represents a mandatory qualification for a number of such strategic positions. Finally, the Academy also runs an MA program in the Prevention and Countering of Terrorism. Although this program is likely to attract some mid-level practitioners from intelligence, security and law enforcement, senior management at the Academy would like to see further international cooperation and training within this realm.30

The number of formal accredited national intelligence and security education programs is rising in other countries too. In 2011, the US formally established the National Intelligence University by expanding the mission of the National Defense Intelligence College. It provides training and education programs from entry level to advanced job-skills, sets curriculum standards, and facilitates the sharing of the intelligence community's training resources.31 Most recently, Germany began setting up a Master's Course in Intelligence and Security Studies at the Federal German University of Applied Administrative Sciences. Although these programs' focus on CT issues varies from nation to nation, this suggests there is growing interest in formalised intelligence and security education across the transatlantic space.

30 '"Mihai Viteazul" National Intelligence Academy'. http://animv.ro/en/despre-noi/, Accessed: 25 April 2017; Interview with Iulian Fota, Director of National Intelligence College, 4 May 2017.

31 Iraq Intelligence Commission. (2005). 'Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction'. Unclassified Version, March, 31, 325-26.

9. Towards a Transatlantic CT Centre of Excellence

The surge in training and educational programs shows that there is a recognised requirement of the benefits increased standardisation and professionalisation can bring, at the domestic and transnational levels. In line with this requirement, our CT CoE proposal aims to contribute in a number of ways. Most crucially, it seeks to create a secure space where CT professionals can discuss best practices. Complimenting this, it aims to accelerate standardisation in terminology, threat assessment, protection of information as well as key tradecraft skills: collection, analysis, and dissemination within CT.

As noted, intelligence cooperation is characterised by a high degree of informality and driven by personal relationships.[32] The proposed CT CoE is not an attempt to change this informal culture. Nevertheless, its establishment is based on the realisation that a critical majority of partners relevant to CT efforts in Europe must work together using common standards and a common understanding of what their intelligence, security, law enforcement and justice communities can and cannot deliver. On a voluntary basis and in cooperation with partners – states, international institutions, academia and even NGOs – the CT CoE would be a platform where best practices are exchanged, syllabuses and training material shared, and relevant courses introduced. With its foundations in a shared perception of threat, and supported by strong political will, the CT CoE's primary goal would be to promote standardisation and build trust and mutual understanding. The added value of joint standardisation and training, which the CoE would design and run, would rest in bringing primarily mid-level intelligence, security and law enforcement professionals together around CT issues to increase trust among participants, and thereby gradually expand the trust in and between their organisations. Once established, the CT CoE could work in concert or informally coordinate with other relevant bodies such as LinCT, the CdB CTG and the growing number of educational institutions devoted to intelligence and security education.

It is clear that as well as a requirement for better standardisation, joint transnational tradecraft training of mid-level CT officers could gradually build capabilities from the bottom up amongst trusted partners. Indeed, during our research, officials indicated that LinCT is interested in developing a CT CoE based around its existing network. Given this potential synergy, and acknowledging GIRI's independence and impartiality, below we present the main proposals for such a body that may prove useful in providing the basis for further consideration for nations.

9.1 CT CoE Framework

The first question that must be addressed is which existing transnational CT network currently has the expertise, trust, capability and respect to host such a new body? While we recognise that for the rapid sharing of operational CT intelligence a core of nations with high degrees of trust, interoperability and capability are needed to ensure secrecy, we believe that for any CoE to add any real value it must include a larger group of nations from the outset. Simultaneously, it must ensure that the utility of the training and education delivered remains collectively beneficial. Given these requirements, LinCT or the CdB's CTG could be the organisation/s within which the CT CoE is initially based. According to some of our interviews, LinCT's close links to the Fives Eyes provides it with the reputation needed to ensure that the training offered is both respected and readily attended by the EU and US CT communities. This reputation extends to non-Five Eyes trusted partners, some of whom already view LinCT meetings as the most desirable and useful to attend due to the frank discussions of best practice. While it is clear that the LinCT is highly respected amongst some European nations, its membership is limited, and for the CT CoE to add real value in terms of common terminology, standards and practices it needs a wider membership in order to uniformly raise capabilities. As such, ideally, the CT CoE will include LinCT and CTG members and both organisations could jointly provide the organisational support or host different programs and courses run under the CT CoE framework. In adopting a joint overarching organisational approach, the CT CoE would become as much a mind set for best practice as a formal training and education centre. Indeed, linking with our Core Transatlantic CT Hub proposal, mandatory membership of the CT CoE for these members would help ensure security culture standards, while the CT CoE could also assess prospective new members of the Hub.

32 Globsec Intelligence Reform Initiative, (2016) Reforming Transatlantic Counter-Terrorism, Bratislava: Globsec, 15.

Another major question is whether the CT CoE should initially be led by a framework nation within LinCT/CTG. Our research revealed a general perception amongst CT professionals with experience of past attempts at transnational CT training that those with a designated framework nation are most successful. This is due to the international trust and reputation associated with a respected nation taking ownership for the project, in liaison with other members. It also shows that a major nation is politically invested in the project for the long run, demonstrating that this nation values it both in operational and political terms and is willing to financially support it. As one CT professional stated, for the CT CoE to succeed, 'it needs true value and positive outcomes. It must be extremely convincing'.[33] As such, within the LinCT/CTG network, potentially nations such as the UK or the Netherlands could take initial ownership of the CT CoE, establishing the syllabi and identifying course locations needed in conjunction with other members. Funding will be an issue, but can be mitigated by the rotation of framework nation every five years or more.

With a framework nation designated within the LinCT/CTG host network, once standardisation and course syllabi have been agreed upon, if desirable, different member states could host different modules. For example, the UK could host a weeklong module; Norway, Germany, Romania and the Netherlands could host others. Such rotation would help spread the administrative and financial burden, but will only be effective if each module remains truly useful. Openness and operational utility must provide the basis for what is delivered in each module.

The Scottish, Norwegian and Romanian examples are interesting as they highlight how academic rigour can be combined with professional expertise to enhance learning and hence capacities. While it will be for any framework nation to decide how to accredit the course, accreditation would act as an enticement for mid-level CT professionals to attend and boost the respectability of the course. In the UK for example, numerous well-respected educational institutions such as Kings' College London, and Warwick and Cranfield Universities have strong links with the intelligence and security services and could potentially accredit the courses and contribute to the syllabi in places of operational utility. Given that the CT CoE could perhaps run four or five week-long modules a year, depending on academic course work and assessment, it is feasible that the level awarded could be a Graduate Certificate or Diploma. Each nation would be expected to send two of their best mid-level CT officers from both the intelligence and law enforcement communities in order to ensure frank discussions, and gradually build trust.

9.2 CT CoE Operational Focus

The CT CoE would primarily drive standardisation at the tactical and operational levels, by encouraging standardisation of terminology, threat assessment, protection of information and privacy as well as key tradecraft skills. This operational level cooperation is critical to the CT CoE: according to Michael Herman, the value of CT intelligence is primarily in its 'nitty-gritty tactical use'.[34] Others have argued that in CT intelligence, more than any other area, tactical data has strategic impact.[35] Recognising the considerable discrepancies between European and transatlantic partners, the raison d'etre of the CT CoE is to get into the 'nitty-gritty' of intelligence and create an environment – both in terms of culture as well as content/training – that enables exchange and harmonisation in a number of areas: terminology, collection, analysis and dissemination.

9.3 Terminology

According to Peter Gill and Mark Phythian, terminology is crucial as it is 'determinative of what, in the end, is considered to be the 'knowledge' upon which policy may be based or by which it is rationalised.' For instance, the subtle differences that intelligence agencies might use to differentiate between different levels of confidence in the intelligence they possess (i.e. 'intelligences shows' vs. 'intelligence indicates'), might escape busy or 'untutored' decision makers. The problem with using non-standardised language in assessments was highlighted in the Butler Report, which stated that

33 Interview, 27 March 2017, Norway.

34 Herman, 2004, 186.

35 Builta, J.A. and Heller, E.N. (2011). 'Reflections on 10 Years of Counterterrorism Analysis'. Institutionalizing Best Practices. Studies in Intelligence, Vol. 55, No. 3, 2.

there was no 'glossary' to define and distinguish between terms such as 'we assess that', 'we judge that', 'we believe that'.[36] This meant that confidence in assessments varied and while this has since been rectified in the UK, such easily solvable issues continue in other states. For example, without a common definition 'probable causes', 'reasonable suspicion' and 'moderate confidence' may mean different things to different CT agencies.

Another relatively simple problem to solve is that of the common formatting of intelligence reports, with information presented in different ways and locations often leading to confusion during routine information and intelligence sharing. Similarly, there is a pressing need to agree upon standardised translations of Arabic names. One of the central goals of the CT CoE would be to act as the focal point for the standardisation of agreed terms for assessment meanings, common language and translation, and formatting. In addressing these relatively solvable issues, the CoE would act as the beacon for the increased operationalisation of information exchange through commonality.

9.4 Collection

Collection, or more precisely the art of accessing intelligence about CT suspects, remains the most difficult area to exchange best practices in as it is highly sensitive and capabilities vary considerably between nations. One important area that the CT CoE should focus on is the introduction of basic tradecraft best practices to raise operational collection capabilities. On the other hand, it must be recognised that major discrepancies in some collection functions will remain. For instance, due to the US' presence in Afghanistan, Iraq and other parts of the Middle East, its CT analysts have been able to utilise intelligence recovered from documents and detainees. Access to such materials has provided the US with both tactical as well as strategic CT intelligence, but such methods have also proved controversial at times.[37] Arguably, European partners' access to such data is more limited, or highly dependent on liaison with Middle Eastern governments or the US. For a number of European nations, whose homeland is the area of operations, they may benefit from exchanging best practices with US colleagues. Nevertheless, understanding best practices in alternative ways of accessing data on terror groups in Europe would be of value to European CT practitioners.

Indeed, one area where a CT CoE could add value is in helping develop a common understanding of when targeted collection is needed. Building on common language and assessments, this could increase the efficiency of collection in some nations and help manage limited resources. This wider setting of the criteria for collection can also be applied to the processes of analysis and dissemination. Similarly, the standardisation of data points for collected information and intelligence is also badly needed. While we recognise that existing national database formats may curtail some CT CoE members from implementing full standardisation, the CoE would be the body that agrees on these standards and provides consultation on standardised database formatting.

9.5 Analysis

The surge in terrorism since 9/11 has dramatically changed analysis requirements.[38] Some have argued, however, that this change was more about the pace rather than the nature of analysis.[39] Two different types of analysis are required within this context; immediate actions to support tactical operations and strategic analysis to understand international events. The Butler Report, which recommended a number of improvements in British intelligence analysis and Joint Intelligence Committee (JIC) assessments, also highlighted this by suggesting staff increases and the establishment of a Professional Head of Intelligence Analysis to advise on methodologies and training. It is highly significant that in the wake of the Butler Report, the British intelligence services, in conjunction with King's College London, have introduced advanced accredited courses specifically for analysts to understand the cognitive/

36 Gill, P. and Phythian, M. (2012). Intelligence in an insecure world. Cambridge: Polity Press, 116-7.

37 Builta and Heller, 2011, 5.

38 Treverton, G. F. and Gabbard, C. B. (2008). Assessing the Tradecraft of Intelligence Analysis. Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/technical_reports/TR293.html, Accessed: 20 April 2017.

39 Marrin, S. (2013). 'Evaluating CIA's Analytic Performance: Reflections of a Former Analyst'. Orbis, 57, 327-8.

functional, historical, structural and political factors that can influence their analysis.[40] In 2005, the Robb Silberman Report, also called for improving the rigor and tradecraft of analysis.

Furthermore, the nature of CT targets calls for increased cooperation between analysts and experts outside of the immediate intelligence and security community, be it geographical, functional or language experts.[41]

9.6 Dissemination

As the process of producing intelligence analysis is not linear, the analyst interacts with users of intelligence at different stages of the process and in different ways in what are often referred to as 'analytic interactions'.[42] A number of classic intelligence-policymaker dissemination models exist, such as 'intelligence brokers' or 'customer liaison staffs', who help interpret policy needs and guide analysts.[43] These dissemination processes influence how analysis is distributed and received by relevant figures in the government. Within the CT context, however, analysts must cater to a number of different users of intelligence, be it policymakers, law enforcement, collectors, military operators or counterparts. This calls not only for an in-depth understanding of the role of these diverse users, but also of CT-specific decision cycles and intelligence requirements of each one of these actors.[44]

Another important dissemination issue the US experienced has been that of the 'threshold' for revealing the identity of a person of interest based upon the threat they pose. This is a result of the legal need to protect information and intelligence until a certain level of threat is reached. Differing privacy laws among CoE member states may limit this in some instances, but agreed common threat terminology will be conducive to developing criteria for revealing suspect identities based on the threat they pose.

9.7 Curriculum

Primarily, the CT CoE should be a secure space where CT intelligence and law enforcement professionals in the European and transatlantic space can share best practice and experiences. Recognising that mid-level CT practitioners are best placed to determine exact course curricula, the following topics are suggested as possible areas to be addressed by the CT CoE.

- **Terminology (setting standards and guidelines for translators from mostly ME languages) and Threat assessment**
- **CT collection methods. To include: target discovery analysis spotting patterns and understanding target behaviors**
- **CT investigations/case management using intelligence**
- **All source CT analysis**
- **Area/ subject studies**
- **Technology**
- **Programming**
- **Advising intelligence consumers**
- **Legal compliance and privacy**

40 Goodman M., and Omand, D. (2008). 'What Analysts Need to Understand: The King's Intelligence Studies Program,' Studies in Intelligence, Vol. 52, No. 4.

41 Builta and Heller, 2011, 8.

42 George, R. Z., and Bruce, J. B. (2014). Analyzing intelligence: origins, obstacles, and innovations. Washington, D.C.: Georgetown University Press, 4.

43 Omand, 2013, 69-70.

44 Builta and Heller, 2011, 8.

Overall, at the transnational level, the closest intelligence networks share common methods and terminology. This report recognises that adopting such common standards is a long-term process that requires a common political and intelligence culture. Furthermore, it acknowledges that it is neither possible nor desirable to dictate the standards of the intelligence, security and law enforcement profession to partner countries. Nevertheless, as discrepancies between states do exist, it is important to understand them and to create a platform for exchanging and potentially adopting practices from different intelligence and security cultures that address the current terrorist threat best.

10. Conclusion

Our CT CoE proposal addresses the wider organisational context of how intelligence agencies and security services innovate and adapt to meet new challenges. Interestingly, how intelligence agencies organisationally transform to face new threats has received limited attention to date, especially outside of the US. There is, however, a long-standing tradition of scholarship on military transformations. While the differences between the intelligence services and the military must be accepted – especially how the need for secrecy can deepen reluctance to change and justify resistance to external criticism – in many respects the military transformation literature is applicable to CT agencies. Broadly speaking, successful transformations have been conceptualised as occurring through two distinct processes: 'top-down' innovation driven by visionary elites; and 'bottom-up' adaption whereby those organisationally closest to the threat evolve to mitigate it.[45] Most importantly for this report, it has been identified how successful transformations have simultaneously included top-down innovation and bottom-up adaption. Indeed, these dual processes have been found to be central to lasting, prevalent organisational change.[46] Interestingly, the most recent scholarship has found that successful military transformations must also reflect the societies from which they are drawn.[47]

Whatever the differences between intelligence and military organisations, given the evolving jihadist threat these concepts of transformation remain important to current debates about intelligence reform. If intelligence agencies do not continuously innovate and adapt to meet the increasingly transnational, criminal and technologically-savvy terrorists of today, the attacks of the past three years will continue. Moreover, by increasing trust amongst core nations' mid-level security personnel, a CT CoE would be conducive to flattening the hierarchical and stove-piped nature of transnational trust frequently concentrated around the most senior personnel. In doing so, this could gradually assist hierarchical intelligence and law enforcement services reflect wider changes in society, whose old hierarchies are widely perceived to be flattening. In short, by targeting adaption from the bottom up, a CT CoE will enable the organic development of a CT network amongst trusted partners.

It is clear therefore that in an ideal situation intelligence reform would simultaneously include top-down innovation and bottom-up adaption. Our previous report's recommendations for a Core CT Hub and Task Forces, and for single search 'hit no-hit' database interfaces are innovations in that they will require politicians, senior policy makers, and in some cases legislators to implement these changes. While we recognise that these are major reforms not without political and organisational risks, we believe that if managed correctly these risks are worth the reward. However, multilateral multi-agency education through a Core CT CoE presents an opportunity to create common standards and language to strengthen collective capability and interoperability. It will also gradually build transatlantic and inter-agency trust in intelligence and law enforcement from the bottom-up. Our CT CoE recommendation is therefore an adaptive change, with low organisational and political risk, and relatively easy to establish in terms of resources and political capital. Thus, promoting standardisation and building trust through regular, formal training and education, and represents the low hanging fruit of transatlantic CT reform: it is the easiest to do, with large potential gains for little risk. Crucially, it provides an opportunity to begin reforming transatlantic CT from the bottom up.

Authors' note:

While conducting research for this feasibility study, dozens of academics, practitioners, and policymakers, both former and current, were consulted and kindly provided helpful insights and guidance. The study also benefited from a number of site visits at institutions which conduct or assist with intelligence education, training or liaison. Due to the sensitive nature of this subject, the majority of our sources have requested to remain anonymous.

45 Posen, B. (1984). The Sources of Military Doctrine. New York: Cornell University Press; Grissom, A. (2006). 'The Future of Military Innovation Studies', Journal of Strategic Studies, 29(5), 910.

46 Foley, R., Griffin, S. and McCartney, H. (2011). '"Transformation in Contact": learning the lessons of modern war', International Affairs, 87(2), 253.

47 Bury, P. (2016). The Transformation of the British Army Reserve, unpublished thesis, University of Exeter.

STRATEGIC PARTNERS OF GLOBSEC

Notes

GLOBSEC
POLICY INSTITUTE

Klariská 14
811 03 Bratislava
Slovak Republic
Phone/Fax: +421 2 5441 06 09
info@globsec.org

www.globsec.org